# 如何確定特定Snort例項處理的流量

## 目錄



## 簡介

本文說明如何確定特定snort例項正在處理的流量。在對特定Snort例項上的CPU使用率較高進行故障排除時，此詳細資訊非常有用。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Firepower技術知識

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Firepower管理中心6.X及更高版本
- 適用於所有受管裝置，包括Firepower威脅防禦、Firepower模組和Firepower感測器

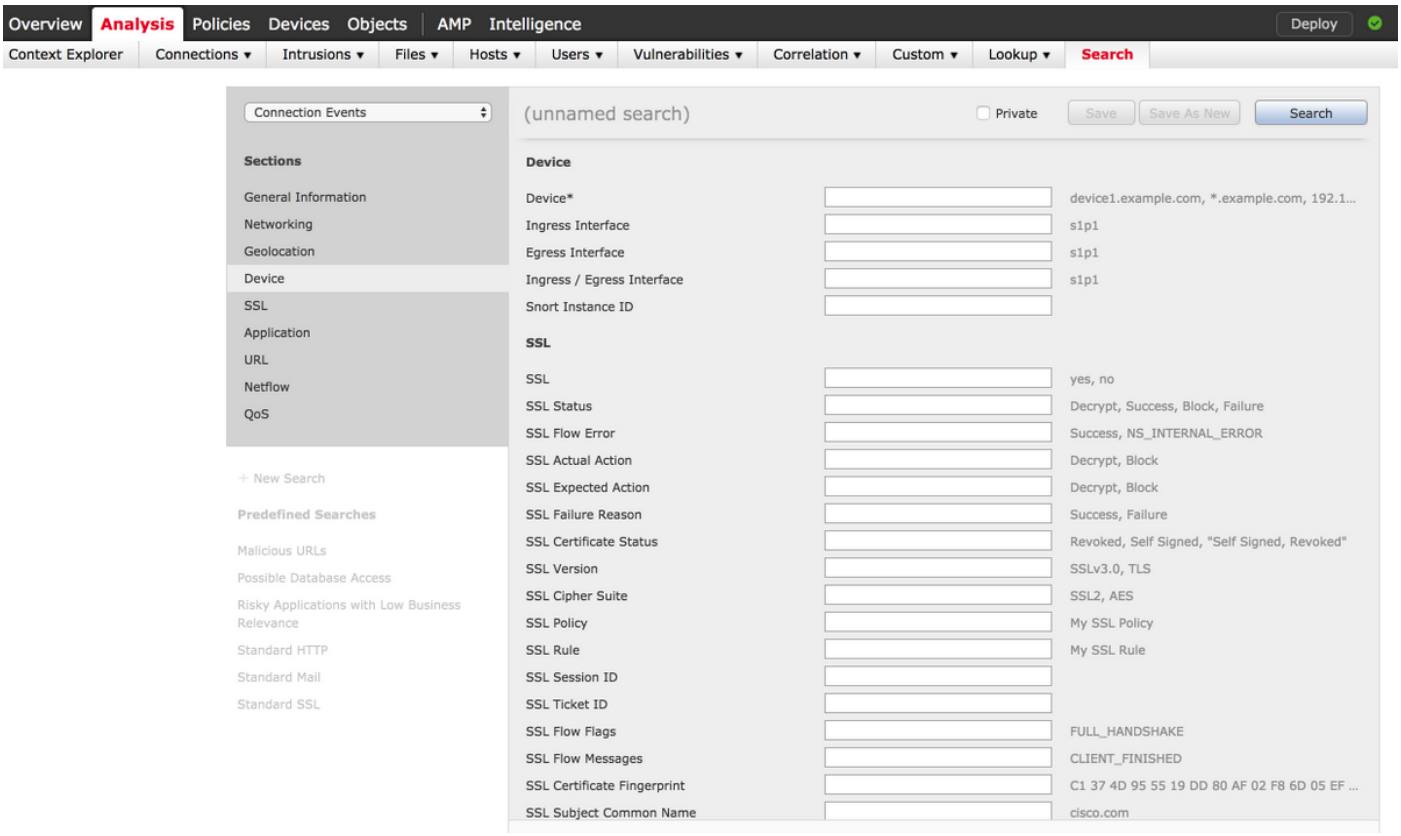
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 設定

### 組態

以管理許可權登入到Firepower管理中心。

登入成功後，導覽至**Analysis > Search**，如下圖所示：




確保從下拉選單中選擇**Connection Events**表，然後從部分中選擇**Device**。為「Device（裝置）」欄位和「Snort Instance ID（Snort例項ID）」輸入值（0到N，Snort例項的數量取決於受管裝置），如下圖所示：


輸入值後，按一下**Search**，結果將是由特定snort例項觸發的連線事件。

**附註**：如果受管裝置是Firepower威脅防禦，則可以使用FTD CLISH模式確定snort例項。

```
> show asp inspect-dp snort
SNORT Inspect Instance Status Info Id Pid Cpu-Usage Conns Segs/Pkts Status tot (usr | sys) -- --
--- ---------------- ---------- ---------- ---------- 0 5266 0% ( 0%| 0%) 0 0 READY 1 5268 0% (
0%| 0%) 0 0 READY 2 5267 0% ( 0%| 0%) 0 0 READY 3 5270 0% ( 0%| 0%) 0 0 READY 4 5269 0% ( 0%|
```

```
0%) 0 0 READY
```

**附註**：如果受管裝置是Firepower模組或Firepower感測器，您可以使用專家模式和基於Linux的**top**命令確定snort例項。

```
admin@firepower:~$ top
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 5247 root      20   0 15248 1272  932 S    0  0.0   0:03.05 top
 5264 root       1 -19 1685m 461m  17m S    0  2.9   1:05.26 snort
```

# 驗證

目前沒有適用於此組態的驗證程序。

# 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。